Советская Белоруссия. – 25.10.2017

Юрий Бакеренко

Определено доменное имя, с которого началось распространение вируса Bad Rabbit

Визначено доменне ім'я, з якого почалося поширення вірусу Bad Rabbit

Компанія в сфері розслідування кіберзлочинів Group-IB визначила доменне ім'я, з якого пішло поширення вірусу-шифрувальника Bad Rabbit. Про це ТАСС розповів гендиректор і основний власник Group-IB Ілля Сачков. За інформацією «Лабораторії Касперського» більшість жертв «Поганого Кролика» знаходиться в Росії, проте схожі атаки також зафіксовані в Україні, Туреччині та Німеччині.

https://www.sb.by/articles/opredeleno-domennoe-imya-s-kotorogo-nachalos-rasprostranenie-virusa-bad-rabbit.html

Компания в сфере расследования киберпреступлений Group-IB определила доменное имя, с которого пошло распространение вируса-шифровальщика Bad Rabbit. Об этом ТАСС рассказал гендиректор и основной владелец Group-IB Илья Сачков.

«Мы определили доменное имя, с которого началось распространение вируса, и с этим доменным именем и IP-адресом связаны еще пять ресурсов», - сказал он.

В Group-IB считают, что злоумышленники могут быть связаны с продажей трафика или привлекли группу из этой сферы. Сачков сообщил, что на владельцев этих сайтов зарегистрировано множество ресурсов, допустим, так называемые «фарм-партнерки» - порталы, которые через спам продают контрафактные лекарства. По словам Ильи Сачкова, группа злоумышленников, которая причастна к хакерской атаке, вероятно, занимается продажей трафика уже несколько лет.

Гендиректор и основной владелец Group-IB полагает, что те данные, которые имеются на данный момент, могут позволить установить причастных к хакерской атаке лиц.

Также Илья Сачков заметил, что атака с помощью Bad Rabbit может носить массовый характер. «Что интересно - преступники поломали достаточно большое количество сайтов, некоторые из которых являются российскими СМИ. Например, «Аргументы.ру», «Фонтанка.ру», «Новая газета Санкт-Петербург». Таким образом, они пытались получить достаточно целевой трафик людей, которые посещают российские сайты», - заключил эксперт в области кибербезопасности.

По информации «Лаборатории Касперского» большинство жертв «Плохого Кролика» находится в России, однако похожие атаки также зафиксированы в Украине, Турции и Германии.

Хакеры используют методы, напоминающие те, что применяли злоумышленники, разработавшие ExPetr.

Пресс-секретарь Microsoft в России Кристина Давыдова рассказала ТАСС, что корпорация изучает информацию о кибератаках.